



**QUEEN'S
UNIVERSITY
BELFAST**

Improving Dynamic Analysis of Android Apps Using Hybrid Test Input Generation

Alzaylaee, M. K., Yerima, S. Y., & Sezer, S. (2017). Improving Dynamic Analysis of Android Apps Using Hybrid Test Input Generation. In International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2017): Proceedings (pp. 1-8). IEEE . DOI: 10.1109/CyberSecPODS.2017.8074845

Published in:

International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2017): Proceedings

Document Version:

Peer reviewed version

Queen's University Belfast - Research Portal:

[Link to publication record in Queen's University Belfast Research Portal](#)

Publisher rights

© 2017 IEEE. This work is made available online in accordance with the publisher's policies. Please refer to any applicable terms of use of the publisher.

General rights

Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy

The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Improving Dynamic Analysis of Android Apps Using Hybrid Test Input Generation

Mohammed K. Alzaylaee, Suleiman Y. Yerima, Sakir Sezer

Centre for Secure Information Technologies (CSIT)

Queen's University Belfast

Belfast, Northern Ireland

Email: {malzaylaee01, s.yerima, s.sezer}@qub.ac.uk

Abstract—The Android OS has become the most popular mobile operating system leading to a significant increase in the spread of Android malware. Consequently, several static and dynamic analysis systems have been developed to detect Android malware. With dynamic analysis, efficient test input generation is needed in order to trigger the potential run-time malicious behaviours. Most existing dynamic analysis systems employ random-based input generation methods usually built using the Android Monkey tool. Random-based input generation has several shortcomings including limited code coverage, which motivates us to explore combining it with a state-based method in order to improve efficiency. Hence, in this paper, we present a novel hybrid test input generation approach designed to improve dynamic analysis on real devices. We implemented the hybrid system by integrating a random based tool (Monkey) with a state based tool (DroidBot) in order to improve code coverage and potentially uncover more malicious behaviours. The system is evaluated using 2,444 Android apps containing 1222 benign and 1222 malware samples from the Android malware genome project. Three scenarios, random only, state-based only, and our proposed hybrid approach were investigated to comparatively evaluate their performances. Our study shows that the hybrid approach significantly improved the amount of dynamic features extracted from both benign and malware samples over the state-based and commonly used random test input generation method.

Index Terms—Android; Malware; Malware detection; Test input generation; DroidBot; Monkey; Code coverage; API calls; Intents

I. INTRODUCTION

Smartphones are becoming an essential electronic device of everyone's daily life. With nearly 80% market share, the Google Android Operating system (OS) is the leading OS in the market compared to iOS, Windows, Blackberry, and Symbian mobile. Over 65 billion downloads have been made from the official Google play store and there are currently more than 1 billion Android devices worldwide [1]. Statista [2] reports there will be more than 1.5 billion Android devices shipped worldwide by 2020. At the same time, malware targeting Android devices has increased significantly over the last few years. According to a report from McAfee, there are around 2.5 million new Android malware samples exposed every year which increased the total number of malware samples discovered in the wild to more than 12 million [3]. Android malware can be found in a variety of applications such as gaming apps, banking apps, social media apps, educa-

tional apps, utility apps etc. Malware-infected apps may have access to privacy-sensitive information, send text messages to premium rate numbers without user approval, or even install a rootkit on the device enabling it to download and execute any code the malware developer wants to deploy etc.

To mitigate the spread of malware, Google introduced Bouncer to its Play store in Feb 2012. Bouncer is the system used to monitor submitted apps for potentially harmful behaviours. It uses a sandbox to test the submitted applications for five minutes in order to spot any malicious activities. However, Bouncer can be evaded by means of some simple detection avoidance techniques [4]. Furthermore, most third party app stores do not have any screening mechanisms for submitted apps. There is therefore a need for efficient detection mechanisms to detect zero-day Android malware in the wild. Several approaches for detecting Android malware have been proposed in previous works. These approaches are categorized into either static or dynamic analysis or utilize both.

In the static analysis approach, the code is usually reverse engineered and examined for presence of any malicious code. [5], [6], [7], [8], [9] are a few examples of detection solutions based on static analysis. While in the dynamic analysis method, the application is executed in a controlled environment, such as a sandbox or virtual machine, or a physical device with the purpose of tracing its behaviour. Researchers have proposed several types of automated dynamic analysis systems to detect suspicious activities and behaviours from Android apps [10], [11], [12], [13], [14], [15], [16]. However, the efficiency of these systems depend on the ability to effectively trigger the malicious behaviours during the analysis.

Android apps are heavily user interface (UI) driven, which makes automated dynamic analysis on smartphones more difficult compared to traditional desktop scenarios. Because of the UI operation, efficient input generation is very important for testing apps and many tools are available to aid developers. Likewise, efficient input generation is needed to drive automated dynamic analysis for malware detection. On the Android platform, malware can hide their malicious activities behind events that require user interaction. Therefore, to test the apps dynamically, researchers need a tool that can simulate the human input to trigger these apps to start their malicious behaviours. The main goal is to reach a high percentage of code coverage such that most of the suspicious activities

are revealed during the analysis. Code coverage refers to the amount of the source code that has been traversed and executed during the dynamic analysis of the apps. Many of the existing dynamic analysis systems such as AppsPlayGround [13], A3E [17], and DynoDroid [18] rely on a random-based input generation strategy based on the Android Monkey UI exerciser tool [19]. According to an empirical study [20], Monkey reached the highest code coverage compared to other test input generation methods. In particular, the study showed that Monkey achieved higher code coverage than more sophisticated test input generation systems like Dynodroid [18], ACTEve [21], A3E [17], GUIRipper [22], SwiftHand [23], and PUMA [24]. Due to the randomness of the inputs generated by Monkey, it may reach certain points in the phone where it is not intended or desired during the dynamic analysis. For example, Monkey could generate inputs that may turn on airplane mode, turn off Wi-Fi, or even turn off the USB debugging mode (which is necessary for device based analysis), etc. All of these will affect the performance of the dynamic analysis tools.

Hence, in order to overcome the aforementioned limitations, we are motivated to explore combining the advantages of different types of test input generation methods to increase the percentage of code coverage as much as possible and potentially collect more dynamic features (API call logs and intents). In this study, we implemented a novel strategy by combining a random-based method (implemented using Monkey [19]) with the state-based method (implemented using DroidBot [25]). Monkey is designed to provide developers with a random testing tool. Whereas DroidBot is a tool designed to intelligently understand the app operation by statistically analysing its code and dynamically analysing the app User Interface (UI) hierarchy. We have implemented the hybrid input generation strategy using python and incorporated this into the DynaLog [16] dynamic analysis tool. Furthermore, in order to validate this approach, we examine the performance of the hybrid method by comparative analysis of Monkey vs. Hybrid, DroidBot vs. Hybrid, Monkey vs. DroidBot, and Monkey vs. DroidBot vs. Hybrid in order to evaluate the performance in terms of number of dynamic API logs and system events collected during analysis. We speculate that the higher the code coverage the more the number of API related features we would be able to extract from the apps. The experiments were performed on real devices using 1222 benign samples from McAfee Labs (Intel Security) and 1222 malware samples from the Android malware genome project [26].

The reminder of the paper is structured as follows. Section II discusses the Android input generation/application triggering tools. Section III details the methodology and experiments undertaken to evaluate the hybrid approach. Section IV presents and discusses the results. Section V discusses the related work, followed by conclusions and future work in Section VI.

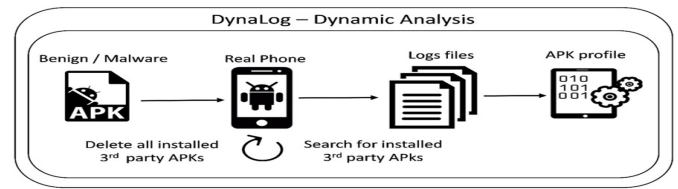


Fig. 1. Phone based feature extraction using DynaLog.

II. TRIGGERING ANDROID APPLICATIONS

As mentioned earlier, there are a number of tools available for dynamic analysis of Android applications. As the main goal is to analyse and detect zero-day malware, there is a need to find the most effective way to ensure adequate code coverage in order to find malicious behaviour with these tools. Android applications can be dynamically analysed by logging API function calls and their response to broadcast events and intents. In order to log these features from the applications at run-time, a platform is needed where an efficient approach to increase the code coverage will also be applied. Since our goal is to perform experiments to compare a random-based, state-based and a hybrid based method on real devices, we need to extract the features in all of these scenarios to make the comparison. Therefore, we applied the DynaLog dynamic analysis framework described in [16] for all the experiments in this paper.

DynaLog is designed to automatically process thousands of applications, starting them sequentially in an emulator or phone, logging several dynamic features and extracting them for further processing. The framework offers the ability to instrument each application with the needed API calls to be observed, logged and extracted during the dynamic analysis. APIMonitor tool [27] was used to build the instrumentation component of DynaLog. It currently relies on the random-based Monkey tool for test input generation. DynaLog framework was extended to be enable device based dynamic analysis as described in [28]. From the results of the study in [28], we utilize this extended version of DynaLog for the experiments presented in this paper using real phones to mitigate the potential impact of anti-emulation and environmental limitations of emulators on our dynamic analysis. Fig. 1 shows an overview of the dynamic analysis process.

A. Random input generation method

Monkey is a random events generator provided as a part of the Android developers' toolkit, which does not require any modification to run. It is also known as an application exerciser tool that sends pseudo-random events of clicks, swipes, touch screens, gestures, etc, to a real device or an emulator. This is to ensure that most of the activities will be traversed to ensure that a high percentage of the application code is covered. In order to start Monkey, the user must to declare the number of events needed to be generated. Once this upper bound is reached, Monkey will be terminated. Monkey can be run with the Android Debug Bridge (adb) tool to test the application

```
pr = subprocess.Popen(["adb", "shell",
    "monkey", "-p", packageName, "-v", "4000", "--throttle 1500",
    "--kill-process-after-error", "-s 500", "28800", "-- ignore-crashes", "-- ignore-
    timeouts", "-- ignore-security-exceptions"],
    stderr = subprocess.PIPE)
```

Fig. 2. Monkey configuration command using adb shell.

and report any errors that are encountered. The basic command to use monkey is as follows:

- *adb shell monkey <options>*

In our experiments, we configure Monkey to run 4000 events for each application and assigned a seed value of 500 for the pseudo-random number generator. The configuration was set to ignore any security exceptions, crashes, or system timeout during the analysis (see Fig. 2). Monkey continues to send events to the application UI until the number of events chosen is reached or until it encounters an error and 'crashes'. From our experience, some of the drawbacks of using Monkey on device based dynamic analysis include:

- The random events generated could lead to turning off the Wi-Fi connection on the phone during the analysis. The Wi-Fi would then remain turned off unless by chance another sequence of random events turns it back on (which is very rare). This situation may hide malicious behaviours that require Internet connection before they can be triggered.
- The random events generated could also turn on the Airplane Mode thus preventing the device from sending or receiving calls, text messages and from connecting to the Internet.
- Monkey could also generate random events that leads to unintended re-configurations of the device and some unwanted behaviour that could affect the analysis. For example, turning off adb debugging from the developer options on the phone which automatically disconnects the phone from the USB connection during analysis.
- Monkey can only generate UI events but not system events [18].
- As it is a random-based input generation tool, Monkey often generates non-relevant events to the current state. These redundant events have no consistent pattern and cannot keep track of events that have already been covered.

To overcome some of the above listed shortcomings of using Monkey in our experiments, we check the status of the Wi-Fi as well as the Airplane mode in order to ensure that they are kept in the desired mode as much as possible throughout the analyses. Fig. 3 Illustrates the code for Airplane mode checking while Fig. 4 shows the code used for checking and restoring the device's Wi-Fi connectivity. The Wi-Fi status is checked prior to starting the analysis of each application and is enabled if it is currently in the disabled state. This capability was implemented using dumpsys, within an adb shell as illustrated in Fig. 4. Two of the keyevents i.e. '19' and '23' are sent via adb shell to turn on the Wi-Fi if it is

```
airPlaneModeStatus = "adb shell settings put global airplane_mode_on 0"
os.system (airPlaneModeStatus)
OFF_AirPlane = "adb shell am broadcast -a
android.intent.action.AIRPLANE_MODE -ez state false"
os.system (OFF_AirPlane)
print("airPlane_Mode is OFF")
```

Fig. 3. Python code to check and restore the Airplane mode in the real phone.

switched off. Note that, in some devices the required keyevent combination could be '20' and '23' instead of '19' and '20'.

B. State-based input generation method

In this study, we used an open source automated test input generation tool known as DroidBot [25] in order to implement a state-based approach. DroidBot is also an Android app exerciser that is considerably smarter than Monkey and can utilize static information extracted from the APK file (e.g. list of sensitive user events) that could be used to improve the event generation. It can avoid redundant re-entry of explored UI states by dynamic UI analysis. Also, DroidBot does not send random gestures (touch, click etc.) like monkey but sends specific gestures according to the position and type of the UI element (unless a 'random' event generation policy is selected). Because of this capability we refer to DroidBot as a 'state-based' generation tool. DroidBot follows four distinct steps when testing an app:

- Connect to a device i.e. emulator or real device.
- Statically analyse the apk using Androguard to infer the list of broadcasts the app may handle and the list of permission the app requires.
- Set up the environment with device usage data like SMS logs, call logs, etc. This is set up according to 'environment policies'.
- Send user events. The events include gestures, broadcasts, key presses, etc., just like the events generated when a user uses the device. Same as setting up environments, DroidBot has multiple policy choices for sending events. For example, static policy is to send app-specific events according to static analysis, and dynamic policy is an extension of the static policy which improves UI event efficiency by dynamically monitoring the UI states. Since we are interested in using DroidBot as a state-based input generator, we chose the 'dynamic' policy configuration during our experiments.

DroidBot also suffers from some limitations. The dynamic policy mode is quite slow as the event state needs to be inferred. Monkey can generate events at a far more rapid pace with the random approach. Even though DroidBot is smarter than Monkey, it is still far less intelligent than manual testing. DroidBot is also unable to deal with unexpected situations, and can get confused by login screens or gets stuck at popup windows and drop-down menus. Since it is not feasible to incorporate manual testing in our automated dynamic analysis of thousands of applications, DroidBot's dynamic approach is perhaps the closest we can get to manual interaction. Since both random-based and the state-based methods have strengths

and drawbacks, we want to obtain the benefits of both by combining their strengths in a hybrid test input generation approach.

C. Hybrid input test method

In this subsection, we discuss our implementation of the hybrid test input generation strategy within the extended DynaLog dynamic analysis framework. As mentioned earlier, DynaLog already relies on Monkey, thus, we need to find a way to integrate DroidBot into the platform. We did this by incorporating a call to invoke a DroidBot instance after Monkey finishes sending its events. Because DroidBot closes the connection with the adb after it finishes, it would not be ideal to start DroidBot before running Monkey. After a number of preliminary tests, we found that Monkey turns on the Airplane modes quite frequently on the devices. This is because the menu was quite easy to reach after a few touches and presses. We also found that the Wi-Fi connection was sometimes turned off as well. Even though we implemented a check for the Airplane mode status at the beginning of each analysis, it will not turn on the Wi-Fi if it has been turned off. Therefore, at the start of each analysis, the Wi-Fi status will be checked as well to make sure it is enabled. These processes will be repeated before and after the running Monkey in order to ensure that the right configuration settings are enabled before DroidBot is started. The process of checking and re-setting the device configurations during the analysis with the hybrid test input generation is illustrated in Fig. 5.

III. METHODOLOGY AND EXPERIMENTS

A. Testbed Setup

The experiments to evaluate the impact of the hybrid test input generation on the dynamic analysis of Android apps were performed using real phones with the following configurations. The phones were: an Elephone P9000 brand equipped with Android 6.0 Marshmallow, Helio P10 MTK6755 Octa Core CPU, 4GB RAM, 4G LTE, 32 GB of ROM, and 32 GB of external SD card storage. Moreover, each phone was installed with a sim card that has some credit to enable sending SMS, outgoing calls, and 3G data usage. The phones also were connected to an internal Wi-Fi access point with internet connection to allow the analysed apps to communicate with their external servers if needed. The analysis was performed in

```
prwifi = subprocess.Popen(["adb", "shell", "dumpsys", "wifi", "|", "grep", "Wi-Fi"],
    stdout=subprocess.PIPE)
wifienabled=True
if prwifi.stdout:
    wifiState=prwifi.stdout.readlines()
    if "disabled" in wifiState[0]:
        wifienabled=False
    if not wifienabled:
        print "now enabling wifi on the device"
        StartWifi= "adb shell am start -a android.intent.action.MAIN -n
            com.android.settings/.wifi.WifiSettings"
        os.system(StartWifi)
        TurnOnWifi1= "adb shell input keyevent 19"
        TurnOnWifi2= "adb shell input keyevent 23"
        os.system(TurnOnWifi1)
        os.system(TurnOnWifi2)
        time.sleep(10)
```

Fig. 4. Python code to check the Wi-Fi status and restore with the connection in the real phone.

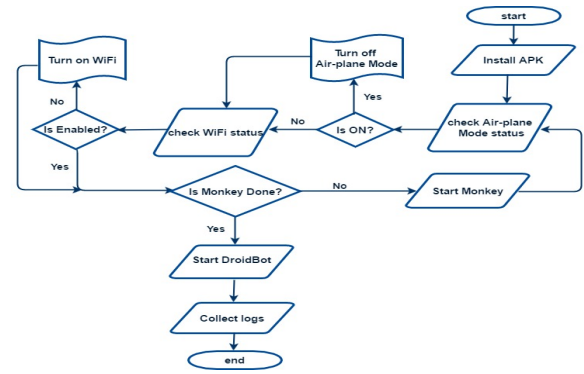


Fig. 5. Checking and restoring device configurations on the hybrid input generation system.

three scenarios. First, all the apps were processed and analysed using Monkey only. Then, they were run again in the analysis environment using DroidBot. Lastly, the system with input test generation from both Monkey and DroidBot together was used to accomplish the hybrid input test generation in the third scenario.

B. App Feature Extraction

Once all the applications are run within the three scenarios, the logs are collected in text files which are further processed into a single .csv file for each scenario. The .csv files contains '0's and '1's symbolizing the presence or absence of each feature being extracted from the log files.

C. Dataset

We have analysed 2444 Android samples in order to extract benign and malware apps' features. Of these, 1222 benign samples were obtained from McAfee Labs (Intel Security). Our malware samples consists of 1222 which belong to 49 Android malware families of the Android malware genome project [26].

IV. RESULTS AND DISCUSSIONS

This section presents the results of the experiments performed to compare the novel hybrid input test generation method with the random-based and state-based standalone methods.

A. Experiment 1: Monkey vs. Hybrid

In order to evaluate the efficiency of the hybrid-based test input generation method, we analysed the extracted features from the scenario with Monkey alone and the scenario with hybrid generation. Table I and Table II show the top-10 extracted features from malware and benign dataset respectively using the hybrid test input compared to the use of Monkey. Both tables show that more features are able to be extracted from the hybrid-based analysis compared to those from the Monkey-based analysis using the same application set. The API method call `Ljava/io/File;->exists`, for instance, was logged from 677 malware APKs using the hybrid test input, while it was only logged from 477 malware APKs using

TABLE I
TOP-10 API CALLS LOGGED FROM MALWARE SAMPLES USING THE
HYBRID METHOD COMPARED TO MONKEY

API signatures	Monkey	Hybrid	Difference
Ljava/io/File;->exists	477	667	190
Ljava/security/MessageDigest;->getInstance	338	473	135
Landroid/content/pm/ApplicationInfo;->getApplicationInfo	435	563	128
Ljava/security/MessageDigest;->digest	310	431	121
Ljava/util/zip/ZipInputStream;->read	219	336	117
Landroid/telephony/TelephonyManager;->getDeviceId	315	429	114
Ljava/util/TimerTask;-><init>	808	921	113
Landroid/content/pm/PackageManager	651	756	105
Lorg/apache/http/client/HttpClient;->execute	89	188	99
Ljava/io/File;->mkdir	274	366	92

TABLE II
TOP-10 API CALLS LOGGED FROM BENIGN SAMPLES USING THE HYBRID
METHOD COMPARED TO MONKEY

API Signatures	Monkey	Hybrid	Difference
Landroid/net/Uri;->parse	192	492	300
Ljava/util/zip/ZipInputStream;->read	173	408	235
Ljava/security/MessageDigest;->digest	297	519	222
Ljava/security/MessageDigest;->getInstance	327	549	222
Lorg/apache/http/client/HttpClient;->execute	56	264	208
Ljava/lang/reflect/Method;->getClass	359	565	206
Ljava/lang/Class;->getName	217	422	205
Landroid/content/Context;->getResources	437	639	202
Ljava/util/TimerTask;-><init>	575	774	199
Landroid/content/pm/PackageManager;->checkPermission	164	359	195

the Monkey-based generation. By the same token, the method *Landroid/telephony/TelephonyManager;->getDeviceId* in Table I, has been extracted from 429 malware APKs using the hybrid method, whereas only 315 malware APKs logged the same API method when Monkey was used.

Similar discoveries appear with the benign samples with even higher differences observed as shown in Table II. With some of the API calls, the difference between the hybrid and Monkey test input generation were >200. For example, the method *Landroid/net/Uri;->parse* was logged from 492 benign APKs using the hybrid method, while the same method was extracted from only 192 benign APKs using Monkey. With dynamic analysis, the malware detection mechanism will likely perform better with more extracted API call features. Overall, the hybrid test input generation shows a much higher efficiency of extracting and logging API calls for the Android applications during the run-time analysis.

B. Experiment 2: DroidBot vs. Hybrid

Table III and Table IV present the top-10 features extracted from both malware and benign samples respectively using the hybrid method vs. DroidBot. With the malware set as in Table III, it can be seen clearly that the hybrid generation allows for the discovery of more API calls with a difference of over 100 in some cases. For instance, the class *Ljava/util/Date* was extracted from only 177 malware samples using DroidBot, while with the hybrid method, it was logged from 124 more malware samples. The differences decreased to less than 20 samples when we applied the same analysis to the benign sample set. Which indicates that DroidBot is far intelligent than Monkey but still is not as efficient as the hybrid method.

C. Experiment 3: Monkey vs. DroidBot

In this subsection, we compare the results from Monkey based analysis to the DroidBot based analysis. In this ex-

TABLE III
TOP-10 API CALLS LOGGED FROM MALWARE SAMPLES USING THE
HYBRID METHOD COMPARED TO DROIDBOT

API signatures	DroidBot	Hybrid	Difference
Ljava/util/Date	177	301	124
Ljava/util/Date;-><init>	171	289	118
Ljava/util/List	171	289	118
Ljava/util/Timer;->schedule	222	339	117
Ljava/util/GregorianCalendar;->getTime	107	207	100
Ljava/util/zip/ZipInputStream;->read	242	336	94
Ljava/io/File;->exists	602	667	65
Ljava/security/MessageDigest;->digest	366	431	65
Lorg/apache/http/client/HttpClient;->execute	133	188	55
Ljava/security/MessageDigest;->update	288	335	47

TABLE IV
TOP-10 API CALLS LOGGED FROM BENIGN SAMPLES USING THE HYBRID
METHOD COMPARED TO DROIDBOT

API signatures	DroidBot	Hybrid	Difference
Landroid/os/Process;->myPid	87	106	19
Landroid/net/Uri;->parse	480	492	12
Landroid/media/AudioManager;->getStreamVolume	37	47	10
Landroid/content/res/AssetManager;->open	320	328	8
Landroid/net/NetworkInfo;->getExtraInfo	23	30	7
Ljava/lang/reflect/Method;->getClass	559	565	6
Landroid/telephony/TelephonyManager;->getSimOperator	72	77	5
Ljava/lang/reflect/Method;->getMethod	245	249	4
Ljava/util/GregorianCalendar;->getTime	188	191	3
Landroid/content/Context;->getAssets	243	246	3

periment, we discovered that some API calls were logged at a higher number with Monkey whereas others were logged at a higher number with DroidBot, using the same sample set. Fig. 6 and Fig. 8 show clearly the differences between Monkey and DroidBot. Fig. 6 illustrates the differences of the extracted features from the malware samples where DroidBot outperforms Monkey. The differences sometimes exceeds 100 for some features extracted from the Malware sample set using DroidBot vs. Monkey. The differences are even higher with the benign sample set. Fig. 7 show the top-10 API calls where DroidBot exceeded Monkey with the benign samples. For example, *Landroid/net/Uri;->parse* was extracted from 480 benign APKs using DroidBot compared to only 192 using Monkey.

In a few exceptional cases, Monkey was better than DroidBot (as shown in Fig. 8) with the malware sample set. More than 100 malware samples logged *Ljava/util/Date;-><init>* using Monkey compare to DroidBot (Fig. 8). This indicates that Monkey, with its random approach, could sometimes reach events that DroidBot may be unable to.

Consequently, we can conclude that even though DroidBot appears to perform better than Monkey in the overall analysis, since in some cases Monkey logs API calls that DroidBot could not, both tools can effectively complement each other. Hence, combining both of them in a hybrid approach makes sense in order to improve code coverage.

Due to the lack of space, we present comparative results for methods form the TelephonyManager class which most malicious apps have been reported to commonly utilize (Fig. 9). The figure shows the overall number of collected API call logs form the three scenarios using the malware sample set. From the figure, it can be seen that the hybrid methods enables more of extraction of the API calls, followed by DroidBot, then Monkey with the lowest performance.

Fig. 10 and Fig. 11 show graphs of comparative perfor-

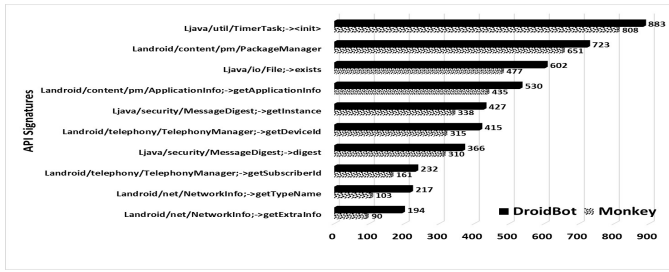


Fig. 6. Top-10 logged API calls from the malware set where DroidBot was better than Monkey.

mance of our proposed hybrid method vs. DroidBot and Monkey for malware and benign samples. Our proposed method exceeded the other two examined input test generation methods in most of the logged API signatures. However, we observed that the overall difference between the hybrid and DroidBot performance is larger in the malware set compared to the benign set as can be seen in the graphs.

From the malware sample set 76 API calls showed differences in numbers between the three methods. The summary of overall findings from the malware sample set are as follows:

- Out of the 76 API calls with differences, 64 of these showed the proposed Hybrid method with higher logs than DroidBot.
- Out of the 76 API calls with differences, 62 showed the proposed Hybrid method having higher logs than Monkey.
- Out of the 76 API calls with differences, 49 showed DroidBot having higher logs than Monkey.
- Out of the 76 API calls with differences, 23 showed Monkey having higher logs than DroidBot.
- Out of the 76 API calls with differences, 10 showed Monkey with higher logs than the proposed Hybrid method.
- Out of the 76 API calls with differences, 4 have DroidBot showing higher logs than the proposed Hybrid method.

From the above summary we can conclude that the hybrid test input generation method surpassed Monkey and the DroidBot methods in overall extraction of API calls from both malware and benign Android applications.

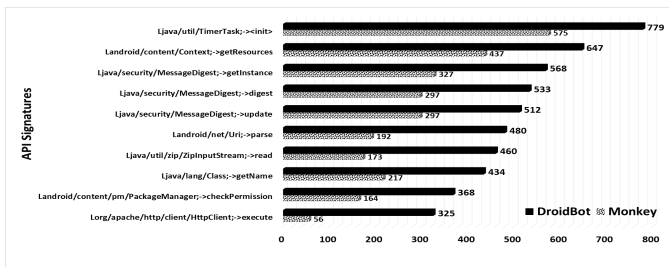


Fig. 7. Top-10 logged API calls from the benign set where DroidBot was better than Monkey.

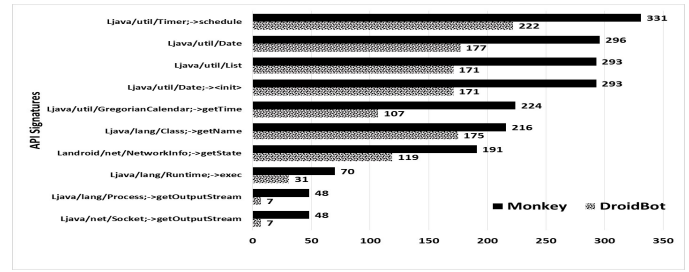


Fig. 8. Top-10 logged API calls from the malware set where Monkey was better than DroidBot.

V. RELATED WORK

Dynamic analysis has been growing in popularity in the field of Android malware detection. Several efforts have been made towards improving the effectiveness of applying Dynamic analysis to detect Android malware. Dynamic analysis uses predefined scripts that will be executed while the application is running in an emulator or real device in order to collect several behaviour indicators. Code coverage is an important factor in dynamic analysis because it determines how much of the malicious behaviour can be discovered. Hence, input generation needs to be as efficient as possible. Contrary to previous work on input test generation approaches or dynamic analysis of Android apps, we attempt to improve the code coverage efficiency by combining a random method using Monkey with state-based method using DroidBot and evaluate the method using real phones. Sophisticated Android malware employ techniques such as reflection, code obfuscation, dynamic loading, and native code which may hinder static analysis tools [29], [30]. Thus, to overcome limitations of static analysis researchers tend to utilize dynamic analysis to investigate the apps during execution. The most popular input test generation tool used in most dynamic analysis systems is Monkey. Monkey [19] is a command-line tool which developers can configure to run on an emulator or real device in order to generate pseudo-random streams of user events such as touches, gestures, or clicks. It is popular due to the simplicity of its configuration and use and is also readily available as part of the Android developers' toolkit. However, the random testing approach may not be so effective in triggering Android malware behaviours. Dynodroid [18] is

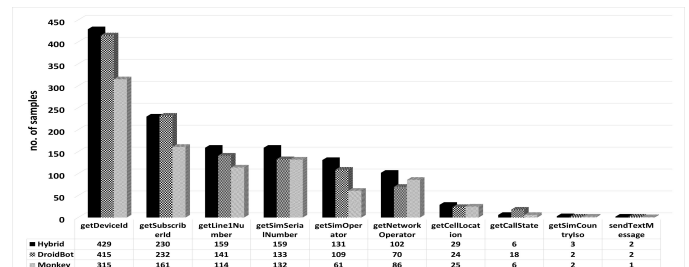


Fig. 9. The overall comparisons of number of the logged methods from TelephonyManager API class using malware sample test.

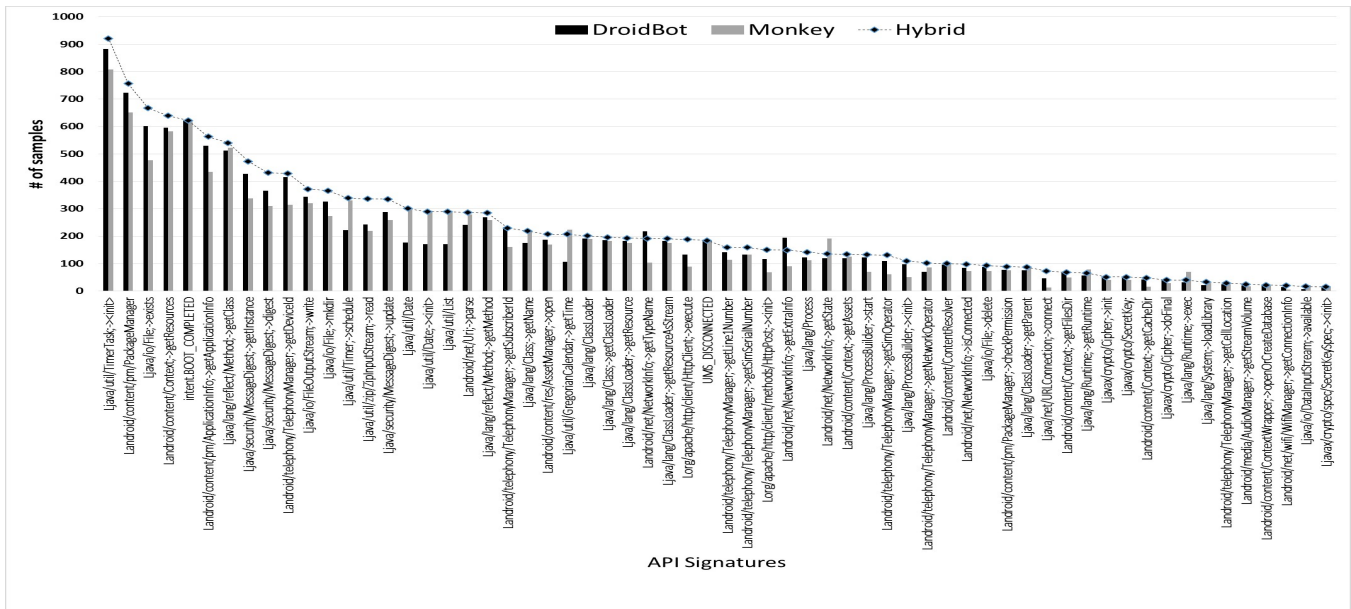


Fig. 10. DroidBot vs. Monkey vs. Hybrid: Number of APKs where logs of the given API calls were found in the malware set.

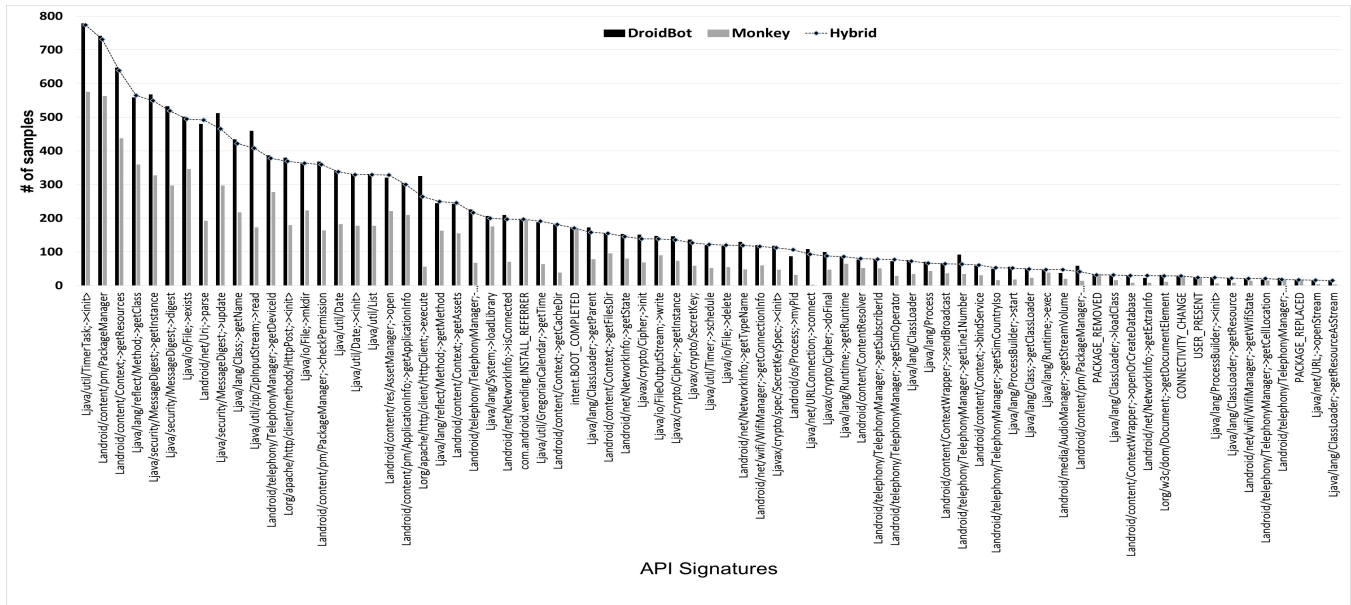


Fig. 11. DroidBot vs. Monkey vs. Hybrid: Number of APKs where logs of the given API calls were found in the benign set.

a random exploration tool that generates both UI inputs and system inputs to Android applications which is based on the principle of observe-select-execute. It also allows combining inputs from machine and human. However, it requires instrumentation of the Android framework in order to generate the system events. It can also run only on an emulator, whereas malware applications can implement anti-emulation techniques in order to avoid detection. Dynodroid restricts the apps from communicating with other apps which may affect the analysis of the malicious apps. A3E [17] is publicly available tool that consists of two strategies to trigger the applications: the DFS

(depth first search) and a taint-targeted approach. However, the open source A3E repository does not provide the taint-targeted strategy. ACTEve [21] is developed to support both system events and UI events which is based on concolic-testing and symbolic execution. However, ACTEve needs to instrument both the Android framework and the application in order to perform the test. An empirical study that evaluates several test input generation tools was done by [20]. It comparatively evaluates Monkey [19], Dynodroid [18], ACTEve [21], A3E [17], GUIRipper [22], SwiftHand [23], and PUMA [24], in terms of the code coverage. The study reveals that

among the tested tools, Monkey performs best on average considering the four measurement metrics used in the study. However, this test was conducted on emulators unlike our work which was performed on real devices. Moreover, this study did not include DroidBot which we used in our study. DroidBot meets our requirements more than other tools because it could run on devices and does not require instrumentation to the Android framework. Unlike the previous works, this paper presents a comparative analysis of a proposed hybrid method that utilizes a combination of random-based and state-based input test generation methods. This is to ensure that more malicious behaviour can be reached and triggered as much as possible due to potentially higher code coverage.

VI. CONCLUSION

In this paper, we presented a novel hybrid test input generation approach that enables us to trigger more malicious behaviours of Android malware during dynamic analysis. We designed and implemented the hybrid strategy to combine a random-based with a state-based input test generation method and incorporated this within a framework that enables automated mass dynamic analysis of applications on real devices. By doing so we are able to leverage the advantages of the random mechanism along with those of the state-based technique to trigger more events and increase the code coverage and hence the possibility of logging more malicious behaviour indicated by API function calls. We have performed several experiments to comparatively evaluate the hybrid strategy with the random and state-based method on real devices and the results shows its capability to trigger more malicious behaviours. The results also showed that several API calls were extracted more effectively from the hybrid test input generation than the single based generation. Thus, we conclude that the use of the hybrid test input generation would improve dynamic analysis code coverage and potentially impact the detection of Android malware. For future work, we propose to evaluate the performance of the hybrid tool using larger sample datasets. Additionally, we intend to evaluate the impact on detection systems that can utilize the API calls collected using the hybrid method for detection of Android malware.

REFERENCES

- [1] Smartphone OS market share worldwide 2009-2015 — Statistic, Statista <https://www.statista.com/statistics/263453/global-market-share-held-by-smartphone-operating-systems>.
- [2] Global smartphone shipments by OS 2016 and 2020 — Statistic, <https://www.statista.com/statistics/309448/global-smartphone-shipments-forecast-operating-system/>.
- [3] McAfee Labs, "McAfee Labs Threats Predictions Report," no. March, pp. 34–35, 2016.
- [4] J. Oberheide and C. Miller, "Dissecting the Android Bouncer," *Summercon 2012*, 2012. [Online]. Available: <http://jon.oberheide.org/files/summercon12-bouncer.pdf>
- [5] S. Y. Yerima, S. Sezer, and I. Muttik, "Android malware detection: An eigenspace analysis approach," in *Science and Information Conference (SAI)*, 2015. IEEE, 2015, pp. 1236–1242.
- [6] D. Arp, M. Spreitzenbarth, H. Malte, H. Gascon, and K. Rieck, "Drebin: Effective and Explainable Detection of Android Malware in Your Pocket," *Symposium on Network and Distributed System Security (NDSS)*, no. February, pp. 23–26, 2014.
- [7] S. Y. Yerima, S. Sezer, and I. Muttik, "High accuracy android malware detection using ensemble learning," *IET Information Security*, vol. 9, no. 6, pp. 313–320, 2015.
- [8] Y. Aafer, W. Du, and H. Yin, "DroidAPIMiner: Mining API-Level Features for Robust Malware Detection in Android," *Security and Privacy in Communication Networks*, vol. 127, pp. 86–103, 2013. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-04283-1_{_}6
- [9] A. Apvrille and T. Strazzere, "Reducing the window of opportunity for android malware gotta catchem all," *Journal in Computer Virology*, pp. 1–11, 2012.
- [10] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones," *Osdi '10*, vol. 49, pp. 1–6, 2010.
- [11] DroidBox, Google Archive <https://code.google.com/archive/p/droidbox/>.
- [12] K. Tam, S. J. Khan, A. Fattori, and L. Cavallaro, "CopperDroid: Automatic Reconstruction of Android Malware Behaviors," *Ndss*, no. February, pp. 8–11, 2015.
- [13] V. Rastogi, Y. Chen, and W. Enck, "AppsPlayground : Automatic Security Analysis of Smartphone Applications," *CODASPY '13 (3rd ACM conference on Data and Application Security and Privacy)*, pp. 209–220, 2013.
- [14] Tracedroid, <http://tracedroid.few.vu.nl/>.
- [15] SandDroid, Hu.Wenjun, <http://sandedroid.xjtu.edu.cn/>.
- [16] M. K. Alzaylaee, S. Y. Yerima, and S. Sezer, "DynaLog: An automated dynamic analysis framework for characterizing android applications," *2016 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2016*, 2016.
- [17] T. Azim and I. Neamtiu, "Targeted and depth-first exploration for systematic testing of android apps," in *ACM SIGPLAN Notices*, vol. 48, no. 10. ACM, 2013, pp. 641–660.
- [18] A. Machiry, R. Tahiliani, and M. Naik, "Dynodroid: An input generation system for android apps," in *Proceedings of the 2013 9th Joint Meeting on Foundations of Software Engineering*. ACM, 2013, pp. 224–234.
- [19] "Ui/application exerciser monkey," Feb 2017. [Online]. Available: <https://developer.android.com/studio/test/monkey.html>
- [20] S. R. Choudhary, A. Gorla, and A. Orso, "Automated test input generation for android: Are we there yet?(e)," in *Automated Software Engineering (ASE), 2015 30th IEEE/ACM International Conference on*. IEEE, 2015, pp. 429–440.
- [21] S. Anand, M. Naik, M. J. Harrold, and H. Yang, "Automated concolic testing of smartphone apps," in *Proceedings of the ACM SIGSOFT 20th International Symposium on the Foundations of Software Engineering*. ACM, 2012, p. 59.
- [22] D. Amalfitano, A. R. Fasolino, P. Tramontana, S. De Carmine, and A. M. Memon, "Using gui ripping for automated testing of android applications," in *Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering*. ACM, 2012, pp. 258–261.
- [23] W. Choi, G. Necula, and K. Sen, "Guided gui testing of android apps with minimal restart and approximate learning," in *ACM SIGPLAN Notices*, vol. 48, no. 10. ACM, 2013, pp. 623–640.
- [24] S. Hao, B. Liu, S. Nath, W. G. Halfond, and R. Govindan, "Puma: Programmable ui-automation for large-scale dynamic analysis of mobile apps," in *Proceedings of the 12th annual international conference on Mobile systems, applications, and services*. ACM, 2014, pp. 204–217.
- [25] HoneyNet, "droidbot," Feb 2017. [Online]. Available: <https://github.com/lynnlyc/droidbot>
- [26] Android Malware Genome Project, Yajin Zhou and Xuxian Jiang, <http://www.malgenomeproject.org/>.
- [27] APIMonitor, <https://github.com/pjlantz/droidbox/wiki/APIMonitor>.
- [28] M. K. Alzaylaee, S. Y. Yerima, and S. Sezer, "Emulator vs real phone: Android malware detection using machine learning," in *Proceedings of the 3rd ACM on International Workshop on Security And Privacy Analytics*, ser. IWSPA '17. Scottsdale, Arizona, USA March 24 - 24, 2017: ACM, 2017, pp. 65–72. [Online]. Available: <http://doi.acm.org/10.1145/3041008.3041010>
- [29] S. Arzt, S. Rasthofer, C. Fritz, E. Bodden, A. Bartel, J. Klein, Y. Le Traon, D. Octeau, and P. McDaniel, "Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps," *Acm Sigplan Notices*, vol. 49, no. 6, pp. 259–269, 2014.
- [30] A. Gorla, I. Tavecchia, F. Gross, and A. Zeller, "Checking app behavior against app descriptions," in *Proceedings of the 36th International Conference on Software Engineering*. ACM, 2014, pp. 1025–1035.